2161

#5
NEW
10-31-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Alain ROSSMANN, et al
Title:	Method and Architecture for Providing Pervasive Security to Digital Assets
Serial No.:	10/076,254
Confirmation No.:	8579
Filing Date:	02/12/2002
Examiner:	N/A
Group Art Unit:	2161
Docket No:	SS-004

June 10, 2002

PETITION TO MAKE SPECIAL UNDER MPEP §708.02 VIII

Assistant Commissioner for Patents
Box Petition Office
Washington, DC 20231

Dear Sir:

The Applicants hereby petition to make the above-referenced application special. The above-referenced application has not received any examination by the Examiner. In accordance with the requirements set forth in the MPEP 708.02 VIII, the applicants submit herewith a Statement of Pre-examination search and Discussion of References Deemed Most Closely Related to Subject Matter Encompassed by the Claims and a copy of each of the related references discussed.

X All the claims in this case are directed to a single invention.

X If the Office determines that all the claims presented are not obviously directed to a single invention, the applicants will make an election without traverse as a prerequisite to the grant of special status.

X If claims 1-14 and 25-38 are found not to be examinable in this case with claim(s) 15 - 24 and 39 - 42, Applicant hereby elects claim(s) 1-14 and 25-38 for the prosecution of this case.

A search has been made by:

the inventor	X Attorney/Agent
X professional searcher	foreign patent office

in the following:

X There is submitted herewith a copy of the references deemed most closely related to the subject matter encompassed by the claims.

X Form PTO-1449 is attached.

X There is submitted herewith a detailed discussion of the references which discussion particularly points out how the claimed subject matter is distinguishable over the references.

X The Commissioner is authorized to charge Deposit Account 502107 an amount of $**130.00** for the Petition herein.

X At any time during the pendency of this application, please charge any fees required or credit any overpayments to Deposit Account 502107.

X Charge the Total Fees due to Deposit Account 502107. At any time during the pendency of this application, please charge any fees required or credit any overpayments to Deposit Account 502107.

Remarks

The applicant respectfully submits that the above statement meets the requirements of MPEP §708.02(VIII) and respectfully request the granting of the

associated petition to make special. Please telephone the undersigned at (408)777-8873, if there are any questions.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Attention: Petition Special, Washington, DC 20231", on June 10, 2002.

Name: JOE ZHENG

Signature: J Zheng

Respectfully submitted;

J Zheng

Joe Zheng
Reg. No.: 39,450

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Alain ROSSMANN, et al
Title:	Method and Architecture for Providing Pervasive Security to Digital Assets
Serial No.:	10/076,254
Confirmation No.:	8579
Filing Date:	02/12/2002
Examiner:	N/A
Group Art Unit:	2161
Docket No:	SS-004

June 10, 2002

STATEMENT OF PRE-EXAMINATION SEARCH AND DISCUSSION OF REFERENCES DEEMED MOST CLOSELY RELATED TO SUBJECT MATTER ENCOMPASSED BY THE CLAIMS

Commissioner for Patents
Box Petition Office
Washington, DC 20231

Dear Sir:

In support of the enclosed Petition to Make Application Special Under MPEP §708.02 VIII, the applicant has requested a pre-examination patent search by a professional search firm in Washington DC. Published patents or patent documents uncovered in the patent search are enclosed herewith. In addition, the applicant(s) has submitted other references that are deemed closely related to the subject matter, or subject matters of the claims.

PTO Form 1449 listing references **A – S3** and **U – V7** is concurrently filed

herewith. The applicant deems these references to be most closely related to the subject matter, or subject matters of the claims:

A. US Patent No.: 4,799,258 to Davies discloses an access control system in which an enciphered message relating to capabilities is stored in the tamper-resistant store of a circuit contained by a token. The store also holds the secret key of a public key encryption system so that the enciphered message and a distinctive message can be transformed ("signed") using the secret key and passed to the computer.

B. US Patent No.: 5,276,735 to Boebert et al a data communication system providing for the secure transfer and sharing of data via a local area network and/or a wide area network. The system includes a secure processing unit which communicates with a personal keying device and a crypto media controller attached to a user's Workstation. The communication between these processing elements generates a variety of data elements including keys, identifiers, and attributes. The data elements are used to identify and authenticate the user, assign user security access rights and privileges, and assign media and device attributes to a data access device according to a predefined security policy. The data elements are manipulated, combined, protected, and distributed through the network to the appropriate data access devices, which prevents the user from obtaining unauthorized data

C. US Patent No.: 5,499,297 to Boebert discloses a system and method for identifying and authenticating users and for controlling the access of those users to privileged instructions within a data enclave. The data enclave includes a plurality of controllers, such as workstations, connected over a network to a security server; each data enclave is assigned a cryptographic key. A personal keying device having an encrypted user unique identifier is assigned to each user; provisions are made for temporarily connecting the personal keying device to one of the controllers and for transmitting an encrypted message, including the user unique identifier and the last

countersign, to the security server to authenticate the user and establish his/her access rights. A mechanism for updating the countersign is provided so that trusted path communications can be established between the user and the security server.

D. US Patent No.: 5,502,766 to Boebert et al. discloses a data communication system providing for the secure transfer and sharing of data via a local area network and/or a wide area network. The system includes a secure processing unit which communicates with a personal keying device and a crypto media controller attached to a user's Workstation. The communication between these processing elements generates a variety of data elements including keys, identifiers, and attributes. The data elements are used to identify and authenticate the user, assign user security access rights and privileges, and assign media and device attributes to a data access device according to a predefined security policy. The data elements are manipulated, combined, protected, and distributed through the network to the appropriate data access devices, which prevents the user from obtaining unauthorized data.

E. US Patent No.: 5,600,722 to Yamaguchi, et al. discloses a cipher communication system and scheme capable of realizing the cipher communication without affecting the already existing application programs and hardware, and establishing a synchronization at the start and end of the cipher communication. In the cipher communication, the session key generated by the key distribution center are obtained and shared at the first and second terminals at a timing of a request for establishing a cipher communication session between the first and second terminals, and then the cipher communication between the first and second terminals is carried out by using the shared session key. The synchronization at the start and end of the cipher communication is established by the matching of the synchronization data transmitted from the first terminal to second terminal or its enciphered form with the return data from the second terminal to the first terminal which is either the synchronization data as received at the second terminal, or its

enciphered form depending on the communication state of the second terminal.

F. US Patent No.: 5,745,573 to Lipner, et al. discloses a system and method for data escrow cryptography are described. An encrypting user encrypts a message using a secret storage key (KS) and attaches a data recovery field (DRF), including an access rule index (ARI) and KS, to the encrypted message. The DRF and the encrypted message are stored in a storage device. To recover KS, a decrypting user extracts and sends the DRF to a data recovery center (DRC) that issues a challenge based on access rules (ARs) originally defined by the encrypting user. If the decrypting user meets the challenge, the DRC sends KS in a message to the decrypting user. Generally, KS need not be an encryption key but could represent any piece of confidential information that can fit inside the DRF. In all cases, the DRC limits access to decrypting users who can meet the challenge defined in either the ARs defined by the encrypting user or the ARs defined for override access.

G. US Patent No.: 5,862,325 to Reed, et al. discloses an automated communications system that operates to transfer data, metadata and methods from a provider computer to a consumer computer through a communications network. The transferred information controls the communications relationship, including responses by the consumer computer, updating of information, and processes for future communications. Information which changes in the provider computer is automatically updated in the consumer computer through the communications system in order to maintain continuity of the relationship. Transfer of metadata and methods permits intelligent processing of information by the consumer computer and combined control by the provider and consumer of the types and content of information subsequently transferred. Object oriented processing is used for storage and transfer of information. The use of metadata and methods further allows for automating may of the actions underlying the communications, including communication acknowledgements and archiving of information.

H. US Patent No.: 5,933,498 to Schneck, et al. discloses a method and device provided for controlling access to data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing a package including: the protected portions of the data and the protected rules. A user is provided controlled access to the distributed data only in accordance with the rules as enforced by a mechanism protected by tamper protection. A device is provided for controlling access to data having protected data portions and rules concerning access rights to the data. The device includes means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.

I. US Patent No.: 5,987,440 to O'Neil, et al. discloses a system for allowing an individual or entity to protect, command, control, and process personal information on a computer network, including the Internet. Specifically, this invention facilitates the formation and use of networked Trusted Electronic Communities, referred to as E-Metro Communities, where each E-Metro Community comprises several members meeting common admission requirements. Preferably, it is the E-Metro Community that sets registration rules and verifies member identity itself or facilitates the use of other trusted Certificate Authorities. The informational identity of each member is encapsulated within the E-Metro Community as electronic personal information agents, referred to as E-PIAs, with each E-PIA representing a member's information and behavior, with some of the

information supplied by each member and some of the information coming from trusted sources external to the member's E-Metro Community. By establishing and enforcing registration rules and performing accountable and audited verifications of member identity, and if so chosen, personal information certification, the E-Metro Community builds a community wherein each of its members can belong and participate in a electronic domain where the rights and responsibilities of privacy and informational self-determination are realized. Thus, it is through the association and certification by a trusted E-Metro Community that a member becomes trusted and reliable in other transactions, but more importantly gains control of their data.

J. US Patent No.: 6,088,717 to Reed, et al. discloses an automated communications system that operates to transfer data, metadata and methods from a provider computer to a consumer computer through a communications network. The transferred information controls the communications relationship, including responses by the consumer computer, updating of information, and processes for future communications. Information which changes in the provider computer is automatically updated in the consumer computer through the communications system in order to maintain continuity of the relationship. Transfer of metadata and methods permits intelligent processing of information by the consumer computer and combined control by the provider and consumer of the types and content of information subsequently transferred. Object oriented processing is used for storage and transfer of information. The use of metadata and methods further allows for automating may of the actions underlying the communications, including communication acknowledgements and archiving of information. Service objects and partner servers provide specialized data, metadata, and methods to providers and consumers to automate many common communications services and transactions useful to both providers and consumers. A combination of the provider and consumer programs and databases allows for additional functionality, including coordination of multiple users for a single database.

K. US Patent No.: 6,088,805 to Davis, et al. discloses methods, systems and computer program products for authenticating a client request to access server resources. A server receives a certificate containing multiple data fields associated with the client making a request. The data fields contain various information related to the requesting client, including the chain of certificate authorities and attributes from their certificates. The server selects data from at least one of the certificate data fields and filters the selected data using at least one predefined filter rule associated with the requested server resources to authenticate the client request. Combinations of filter rules may be utilized and the server may select data from various combinations of data fields.

L. US Patent No.: 6,098,056 to Rusnak, et al. discloses a system and method for limiting access to and preventing unauthorized use of an owner's digital content stored in an information network and available to clients under authorized conditions. The network includes at least one server coupled to a storage device for storing the limited access digital content encrypted using a random-generated key, known as a Document Encryption Key (DEK). The DEK is further encrypted with the server's public key, using a public/private key pair algorithm and placed in a digital container stored in a storage device and including as a part of the meta-information which is in the container. The client's workstation is coupled to the server for acquiring the limited access digital content under the authorized condition. A Trusted Information Handler (TIH) is validated by the server after the handler provides a data signature and type of signing algorithm to transaction data descriptive of the purchase agreement between the client and the owner. After the handler has authenticated, the server decrypts the encrypted DEK with its private key and re-encrypts the DEK with the handler's public key ensuring that only the information handler can process the information. The encrypted DEK is further encrypted with the client's public key personalizing the digital content to the client. The client's program decrypts the DEK with his private key and passes it along with the encrypted content to the handler which decrypts the

DEK with his private key and proceeds to decrypt the content for displaying to the client.

M. US Patent No.: *6,158,010* to Moriconi, et al. discloses a system and method for maintaining security in a distributed computing environment comprises a policy manager located on a server for managing and distributing a security policy, and an application guard located on a client for managing access to securable components as specified by the security policy. In the preferred embodiment, a global policy specifies access privileges of the user to securable components. The policy manager may then preferably distribute a local client policy based on the global policy to the client. An application guard located on the client then manages access to the securable components as specified by the local policy.

N. US Patent No.: 6,161,139 to Win, et al. discloses a method that comprises storing information that defines administration roles, that associates a user with one or more of the administrative roles, and that associates each administration role with one or more administrative privileges. An administrative privilege authorizes at least one administrative function. When the user requests the execution of an administrative function, the requests is honored only when one of the user's administrative roles includes an administrative privilege that authorizes the requested administrative function. In addition, information is stored that associates each of a plurality of users with one or more administrative roles. At least two users administer the access control computer system from different locations, or from computers connected to two different local area networks. Information associating a user with one or more administrative roles may be stored in a cookie, which may be encrypted. The information stored in the cookie is used to determine whether an administrative function requested by a user may be executed on behalf of the user.

O. US Patent No.: 6,182,142 B1 to Win, et al. discloses a method for controlling access to information resources, a single secure sign-on gives the

user access to authorized resources, based on the user's role in the organization. The information resources are stored on a protected server. A user of a client or browser logs in to the system. A runtime module on the protected server receives the login request and intercepts all other request by the client to use a resource. The runtime module connects to an access server that can determine whether a particular user is authentic and which resources the user is authorized to access. User information is associated with roles and functional groups of an organization to which the user belongs; the roles are associated with access privileges. The access server connects to a registry server that stores information about users, roles, functional groups, resources, and associations among them. The access server and registry server exchange encrypted information that authorized the user to use the resource. The access server passes encrypted tokens that define the user's roles and authorization rights to the browser or client, which stores the tokens in memory. The user is presented with a customized display showing only those resources that the user may access. Thereafter, the access server can resolve requests to use other resources based on the tokens without contacting the registry server.

P. US Patent No.: 6,226,745 B1 to Wiederhold discloses a security mediator system used in a computer system having a database of information to be shared with authorized users in accordance with pre-defined constraints. A rules database stores rules, including query pre-processing rules and query results post-processing rules. The rules database includes data for specifying, for each of a plurality of specified groups of users, which of the rules in the rules database are applicable to queries received from users in each of the groups. A query pre-processing module applies to each received query all pre-processing rules in the rules database applicable to the query in accordance with the identified user who submitted the query. If any applicable rule is not passed, the query is blocked; otherwise execution of the query is enabled. A database access module executing each enabled query to produce a corresponding result. A post-processing module applies to the

results all post-processing rules in the rules database applicable to the executed query. If any applicable rule is not passed, transmission of the results is blocked; otherwise transmission of the results to the identified user is enabled. A security officer module processes blocked queries and blocked results, enabling a security officer to review blocked queries and blocked results, and to either confirm the blocking determination or override it.

Q. US Patent No.: 6,249,873 B1 to Richard, et al. discloses a system in which a server receives the client's Distinguishing Name (DN), and then searches its directory for identification information and access control rights for this specific context. The server can act as a stand-alone server or in conjunction with other directory services on the network. A client must have a verifiable identity in order for secure communications to continue. A client's identity can be said to be fully verifiable if the server has access to the directory service that maintains that client's DN. The client receives the server's DN, and the client can then determine whether or not to accept a response to a request for information (i.e., trust the response). The client determines the identity of the server using some directory service (the client can act stand-alone or as a client of other directory servers). A server is fully verifiable if the client can identify the directory service that maintains the server's DN. In both cases, determining identity is predicated on being able to identify a directory service.

R. US Patent No.: 6,272,631 B1 to Thomlinson, et al. a central storage architecture for core data secrets, referred to as data items. The architecture includes a storage server, a plurality of installable storage providers, and one or more authentication providers. Programming interfaces are exposed so that application programs can utilize the services provided by the invention without having to actually implement the features. When storing a data item using the protected storage services, an application program can specify rules that determine when to allow access to the data item. Access can, if desired, be limited to the current computer user. Access can similarly be limited to specified application programs or to certain classes of application

programs. The storage server authenticates requesting application programs before returning data to them. A default authentication provider authenticates users based on their computer or network logon. A default storage provider allows storage of data items on magnetic media such as a hard disk or a floppy disk. Data items are encrypted before they are stored. The encryption optionally uses a key that is derived from the previous authentication of the user. Specifically, the key is derived from the user's password, supplied during logon. In addition, an application program or the user can specify that certain items require another password that is entered whenever access to the data is requested. The default storage provider implements a multi-level encryption scheme to minimize the amount of encryption that has to be re-done when the user changes a password. Each data item is encrypted using an item key that is generated randomly by the system. The item key is in turn encrypted with a master key that is itself encrypted with a key derived from the user-supplied password (such as the user's logon password).

S. US Patent No.: 6,272,632 B1 to Carman, et al. discloses a system and method for data recovery. In one embodiment, an encrypting system encrypts a message or file using a secret key (KS) and attaches a key recovery field (KRF), including an access rule index (ARI) and KS, to the encrypted message or file. To access the encrypted message or file, a decrypting system must satisfactorily respond to a challenge issued by a key recovery center. The challenge is based on one or more access rules that are identified by the ARI included within the KRF.

S1. US Patent No.: 6,289,450 B1 to Pensak, et al. discloses a system for encrypting electronic information such as a document so that only users with permission may access the document in decrypted form. The process of encrypting the information includes selecting a set of policies as to who may access the information and under what conditions. A remote server stores a unique identifier for the information and associates an encryption/decryption key pair and access policies with the information. Software components residing on the author's computer retrieve the encryption key from the remote

server, encrypt the information, and store the encrypted information at a location chosen by the author. A user wishing to access the information acquires the encrypted information electronically. Software components residing on the viewing user's computer retrieve the associated decryption key and policies, decrypt the information to the extent authorized by the policies, and immediately delete the decryption key from the viewing user's computer upon decrypting the information and rendering the clear text to the viewing user's computer screen. The software components are also capable of prohibiting functional operations by the viewing user's computer while the clear text is being viewed.

S2. US Patent No.: 6,314,409 B2 to Schneck, et al. discloses techniques for controlling access to data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing a package including: the protected portions of the data and the protected rules. A user is provided controlled access to the distributed data only in accordance with the rules as enforced by a mechanism protected by tamper protection. A device is provided for controlling access to data having protected data portions and rules concerning access rights to the data. The device includes means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.

S3. US Patent No.: 6,339,825 B2 to Pensak, et al. discloses a system for encrypting electronic information such as a document so that only users with

permission may access the document in decrypted form. The process of encrypting the information includes selecting a set of policies as to who may access the information and under what conditions. A remote server stores a unique identifier for the information and associates an encryption/decryption key pair and access policies with the information. Software components residing on the author's computer retrieve the encryption key from the remote server, encrypt the information, and store the encrypted information at a location chosen by the author. A user wishing to access the information acquires the encrypted information electronically. Software components residing on the viewing user's computer retrieve the associated decryption key and policies, decrypt the information to the extent authorized by the policies, and immediately delete the decryption key from the viewing user's computer upon decrypting the information and rendering the clear text to the viewing user's computer screen. The software components are also capable of prohibiting functional operations by the viewing user's computer while the clear text is being viewed.

U. & V0. "Inside Encrypting File System", Part 1 and Part 2, disclose what is commonly known as Encrypting File System (EFS) in Microsoft Windows OS. EFS uses a file encryption key to encrypt the file's contents with a stronger variant of the Data Encryption Standard (DES) algorithm-DESX. EFS stores the file's FEK with the file but encrypts the file with the user's EFS public key using the RSA public key-based encryption algorithm. After EFS completes these steps, a secured file is generated.

V1. "Security with Encrypting File System" discloses Encrypting File System (EFS) that uses an encryption attribute to designate files for EFS protection. When a file's encryption attribute is on, EFS stores the file as encrypted ciphertext. When an authorized user opens an encrypted file in an application, EFS decrypts the file in the background and provides a plaintext copy to the application. The authorized user can view or modify the file, and EFS saves any changes transparently as ciphertext. Other users are denied permission to view or modify EFS-encrypted files. EFS-protected files are

bulk encrypted to provide confidentiality even from intruders who bypass EFS and attempt to read files by using low-level disk tools.

V2. "How EFS Works" discloses Encrypting File System (EFS) that uses public key encryption in conjunction with symmetric key encryption to provide confidentiality for files that resists all but the most sophisticated methods of attack. The file encryption key (a symmetric bulk encryption key) is used to encrypt the file and is then itself encrypted by using the public key taken from the user's certificate, which is located in the user's profile. The encrypted FEK is stored with the encrypted file and is unique to it. To decrypt the FEK, EFS uses the encryptor's private key, which only the file encryptor has.

V3. "Encrypting File System" also explains how Encrypting File System (EFS) works. Namely it encrypts a file using a symmetric encryption key unique to each file. Then it encrypts the encryption key using a public key from the file owner's EFS certificate. Since the file owner is the only person with access to the private key, that person is the only one who can decrypt the key, and therefore the file.

V4. "Features of EFS" describes some features commonly known about Encrypting File System (EFS), it further lists that: EFS only works on the Windows 2000 NTFS file system; EFS does not run if there is no recovery agent certificate, but it does designate a recovery agent account by default and generates the necessary certificate if you do not; you can use EFS to encrypt or decrypt data on a remote computer, but you cannot use it to encrypt data sent over the network; you cannot encrypt system files or folders; you cannot encrypt compressed files and folders until you decompress them; encrypting an entire folder ensures that the temporary copies of encrypted files that it contains are also encrypted; copying a file into an encrypted folder encrypts the file, but moving it into the folder leaves the file encrypted or unencrypted, just as it was before you copied the file; moving or copying EFS files to another file system removes the encryption, but backing them up preserves the encryption; other file permissions are

unaffected, an administrator, for instance, can still delete a user's EFS file even though the user cannot open it.

V5. "Windows 2000 EFS" provides a brief description of Encrypting File System (EFS) in view of NT and UNIX systems relying on a discretionary access control (DAC) system.

V6. US Patent Application No.: 2001/0021926A1 to Schneck et al discloses techniques for controlling access to data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing a package including: the protected portions of the data and the protected rules.

V7. US Patent Application No.: 2002/0010679 A1 to Felsher provides a trustee model for the collection, maintenance and distribution of entrusted information content, such as medical records or copyright works. Medical institutions and individuals are responsible for creating and storing medical records for patients treated. These medical institutions are the custodians of the records, over which the patient, or the successors of the patient hold rights. One of the patient's rights is the right to control release of the records.

However, the claimed subject matter is distinguishable with particularity over the above patents/publications by:

Claim 1's "establishing a secured link with a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data,

wherein the electronic data is secured in a format including security information and an encrypted data portion, the security information including access rules and controlling restrictive access to the encrypted data portion; authenticating the user according to the identifier; and activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information."

Claim 20's "authenticating a user attempting to access the electronic data; maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when and where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme; encrypting the security information with the public key when the electronic data is to be written into a store; and decrypting the security information with the private key when the electronic data is to be accessed by an application."

Claim 31's "receiving a request to access the electronic data; determining security nature of the electronic data; when the security nature indicates that the electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme, determining from the security information if the user has necessary access privilege to access the encrypted data portion; and decrypting the encrypted data portion only after the user is determined to have the necessary access privilege to access the encrypted data portion."

Claim 41's "a client machine executing a document securing module that operates in a path through which the electronic data is caused to pass when selected, the document securing module determining security nature of the electronic data, an

access control server coupled to the client machine over a network, the access control server including an account manager managing all users who access the electronic data; and wherein the client machine and a user thereof are caused by the document securing module to be authenticated with the access control server when the security nature indicates that the electronic data is secured; and wherein access rules in the secured electronic data are retrieved with a user key associated with the user."

Claim 47's "a storage device including at least an active place designated for keeping the electronic data secured, the secured electronic data including encrypted security information that further includes at least a set of access rules and a file key, wherein the access rules, expressed in a descriptive language, protects the file key and controls restrictive access to the secured electronic data; a client machine coupled to the storage device and executing a document securing module operative to intercept the electronic data when the electronic data is caused to transport from the active place; an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data after both the user and the client machine are authenticated; wherein the set of access rules are measured against access privilege of the user in the access control server, if successful, the file key is returned to the client machine to facilitate a recovery of the electronic data in clear mode."

Claim 48's "program code for establishing a secured link with a client machine when an authentication request is received therefrom, the authentication request including an identifier identifying a user from the client machine to access the electronic data in a secured format including security information and an encrypted data, the security information including access rules and controlling restrictive access to the encrypted data portion; program code for authenticating the user according to the identifier; and program code for activating a user key

after the user is authenticated, wherein the user key is used to access the access rules in the security information."

Claim 67's "program code for authenticating a user attempting to access the electronic data; program code for maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling restrictive access to the encrypted data portion and protecting the private key and a public key by access rules therein; program code for encrypting the security information with the public key when the electronic data is to be written into a store; and program code for decrypting the security information with the private key when the electronic data is to be accessed by an application."

Claim 78's "program code for receiving a request to access the electronic data; program code for determining security nature of the electronic data; when the security nature indicates that the electronic data is secured, wherein the electronic data including a header and an encrypted data portion, the header including security information and the encrypted data portion is an encrypted version of the electronic data according to a predetermined encryption scheme, program code for determining from the security information if the user has necessary access privilege to access the encrypted data portion; and program code for decrypting the encrypted data portion only after the access privilege of the user is permitted in view of the security information."

Hence, the applicant believes that claims 1, 20, 31, 41, 78, 48, 67, and 78 and thus their dependent claims also, are each patentable over the references discussed and listed in paragraph A-V7 above.

Please telephone the undersigned at (408)777-8873, if there are any questions.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", on June 10, 2002.

Name: Joe Zheng

Signature: J Zheng

Respectfully submitted;

J Zheng

Joe Zheng
Reg. No.: 39,345

Form PTO-1449 (Modified)	Atty Docket No.: SS-004	Application No.: 10/076,254
List of Patents and Publications Statement (Use several sheets if necessary)		Applicant: Alain ROSSMANN
		Filing Date: 02/12/2002

REFERENCE DESIGNATION		U.S. PATENT DOCUMENTS					
Examiner Initials		Document No.	Date	Patentee	Class	Sub-Class	Filing date if appropriate
F.B.	A.	4,799,258	Jan. 17, 1989	Davies	380/21		02/07/1985
	B.	5,276,735	Jan. 4, 1994	Boebert et al.	380/21		04/17/1992
	C.	5,499,297	Mar. 12, 1996	Boebert	380/23		12/20/1994
	D.	5,502,766	Mar. 26, 1996	Boebert et al.	380/25		10/26/1993
	E.	5,600,722	Feb. 4, 1997	Yamaguchi et al.	380/21		10/06/1993
	F.	5,745,573	Apr. 28,1998	Lipner et al.	380/21		01/10/1997
	G.	5,862,325	Jan. 19, 1999	Reed et al.	395/200.31		09/27/1996
	H.	5,933,498	Aug. 3, 1999	Schneck et al.	380/4		11/05/1997
	I.	5,987,440	Nov. 16, 1999	O'Neil et al.	705/44		07/22/1997
	J.	6,088,717	Jul. 11, 2000	Reed et al.	709/201		08/31/1998
	K.	6,088,805	Jul. 11, 2000	Davis et al.	713/202		02/13/1998
	L.	6,098,056	Aug. 1, 2000	Rusnak et al.	705/75		11/24/1997
	M.	6,158,010	Dec. 5, 2000	Moriconi et al.	713/201		02/12/1999
	N.	6,161,139	Dec. 12, 2000	Win et al.	709/229		02/12/1999
	O.	6,182,142 B1	Jan. 30, 2001	Win et al.	709/229		07/10/1998
	P.	6,226,745 B1	May 1, 2001	Wiederhold et al.	713/200		03/16/1998
	Q.	6,249,873 B1	Jun. 19, 2001	Richard et al.	713/200		07/13/1999
	R.	6,272,631 B1	Aug. 7, 2001	Thomlinson et al.	713/155		06/30/1997
	S.	6,272,632 B1	Aug. 7, 2001	Carmen et al.	713/168		02/12/1998
	S1.	6,289,450 B1	Sep. 11, 2001	Pensak et al.	713/167		05/28/1999
	S2.	6,314,409 B2	Nov. 6, 2001	Schneck et al.	705/54		10/26/1998
F.B.	S3	6,339,825 B2	Jan. 12, 2002	Pensak et al.	713/158		07/18/2001

FOREIGN PATENT DOCUMENTS

Examiner Initials		Document No.	Date	Country	Class	Sub-Class	Trans-lation
	T0.						
	T1.						
	T2.						
	T3.						
	T4.						

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)

Examiner Initials		Publication Details
F.B.	U	"Inside Encrypting File System", Part 1, from MSDN October, 2001 version, exact publication date is unknown but believed prior to 12/12/2001.
	V0.	"Inside Encrypting File System", Part 2, from MSDN October, 2001 version, exact publication date is unknown but believed prior to 12/12/2001.
	V1.	"Security with Encrypting File System", from MSDN October, 2001 version, exact publication date is unknown but believed prior to 12/12/2001.
	V2.	"How EFS Works", from MSDN October, 2001 version, exact publication date is unknown but believed prior to 12/12/2001.
	V3.	"Encrypting File System", from MSDN October, 2001 version, exact publication date is unknown but believed prior to 12/12/2001.
	V4.	"Features of EFS", from MSDN October, 2001 version, exact publication date is unknown but believed prior to 12/12/2001.
	V5.	" Windows 2000 EFS", in the April 1999 issue of *Windows NT Magazine*
	V6.	Schneck et al, "System for controlling access and distributing of digital property", US Patent Publication, Sep. 13, 2001, US2001/0021926A1.
F.B.	V7.	Felsher "Information record infrastructure, system and method", US Patent Application, Jan. 24, 2002, US2002/0010679A1
	V8.	
	V9.	

Examiner	Date Considered
[signature]	5/6/03

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to the applicant.